(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－285283
（P2001－285283A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/32		Ｇ０９Ｃ	1/00	６６０Ｅ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｌ	9/00	６７３Ａ　５Ｋ０３０
Ｈ０４Ｌ	9/08				６０１Ｄ　５Ｋ０３３
	12/28			11/00	３１０Ａ　９Ａ００１
	12/66			11/20	Ｂ

審査請求　未請求　請求項の数13　ＯＬ　（全９頁）

(21)出願番号　特願2000－94840(P2000－94840)

(22)出願日　平成12年３月30日(2000.3.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号

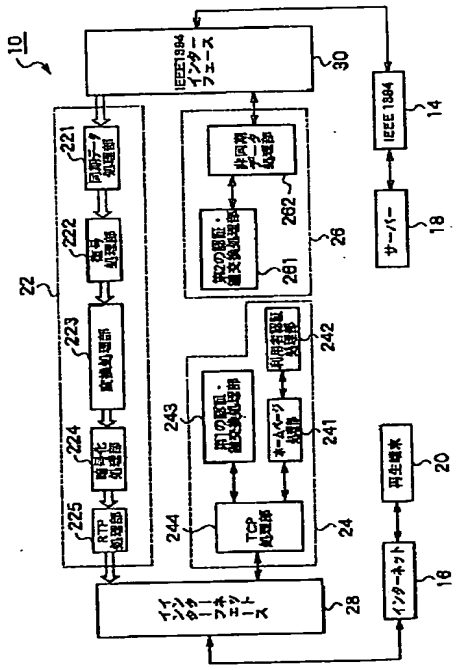
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　通信装置およびその通信方法

(57)【要約】
【課題】　家庭網から公衆網へデータを送信する際の著作権保護を実現する通信装置およびその通信方法を提供する。
【解決手段】　インターネット等の公衆網１６とIEEE1394等の家庭網１４を結ぶ通信装置である。この通信装置は、公衆網１６に接続された再生端末２０との間で、認証・鍵交換を実行する第１の認証・鍵交換処理部２４３と、家庭網１４に接続されたサーバー１８との間で、認証・鍵交換を実行する第２の認証・鍵交換処理部２６１と、サーバー１８から得られた、著作権保護のために暗号化されたAVデータを、再生端末２０に送信する送信部２２と、再生端末２０の利用者を認証し、その利用者の認証ができない場合には、再生端末２０との通信を拒絶する利用者認証処理部２４２と、から構成される。



1

【特許請求の範囲】

【請求項１】　公衆網である第１の網とローカルエリアネットワークである第２の網の間に配置され、該第１の網に接続された第１の端末と該第２の網に接続された第２の端末の間で暗号化データを転送する通信装置であって、

前記第１の端末との間で、認証・鍵交換を実行する第１の認証・鍵交換部と、

前記第２の端末との間で、認証・鍵交換を実行する第２の認証・鍵交換部と、

前記第２の端末から得られた暗号化データに、所定の変換を施し、かつ該データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、前記第１の端末に送信する送信部と、

前記第１の端末の利用者を認証し、該利用者の認証ができない場合には、前記第１の端末との通信を拒絶する利用者認証部とを有することを特徴とする通信装置。

【請求項２】　前記第１の認証・鍵交換部は、前記第１の端末からの、前記第２の端末に対するデータ送信要求を、前記第２の端末に通知する手段を備える、ことを特徴とする請求項１に記載の通信装置。

【請求項３】　前記送信部は、前記第２の端末から得られた暗号化データを復号する手段、該復号されたデータに対して前記所定の変換を施す手段、および、該変換されたデータを暗号化する手段、を備える、ことを特徴とする請求項１に記載の通信装置。

【請求項４】　前記変換手段は、データ圧縮符号化方式およびデータ圧縮符号化速度のうちの少なくとも一方を変換する、ことを特徴とする請求項３に記載の通信装置。

【請求項５】　前記利用者認証部は、正規の利用者の識別ＩＤおよび該識別ＩＤに対応するパスワードをあらかじめ登録する利用者情報登録手段を備える、ことを特徴とする請求項１に記載の通信装置。

【請求項６】　前記第２の端末に通知する手段は、前記第１の端末の利用者の認証ができた場合のみ、前記第１の端末からのデータ送信要求を受付ける、ことを特徴とする請求項２に記載の通信装置。

【請求項７】　前記第１の認証・鍵交換部は、前記第１の端末の利用者の認証ができた場合のみ、前記第１の端末との間の認証・鍵交換を実行する、ことを特徴とする請求項１に記載の通信装置。

【請求項８】　公衆網である第１の網に接続された第１の端末とローカルエリアネットワークである第２の網に接続された第２の端末との間で暗号化データを転送する通信方法であって、

前記第１の端末の利用者を認証する工程と、

該利用者の認証ができた場合のみ、前記第２の端末から暗号化データを取得する工程と、

該取得された暗号化データに、所定の変換を施し、かつ該データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、前記第１の端末に送信する工程とを含むことを特徴とする通信方法。

2

【請求項９】　前記利用者を認証する工程は、前記利用者から識別ＩＤおよび該識別ＩＤに対応するパスワードを取得するステップ、および、該取得された識別ＩＤおよびパスワードが、あらかじめ登録された、正規の利用者の識別ＩＤおよび該識別ＩＤに対応するパスワードと、一致するか否かを照合するステップ、を含むことを特徴とする請求項８に記載の通信方法。

【請求項１０】　前記第１の端末に送信する工程は、前記第２の端末から得られた暗号化データを復号するステップ、該復号されたデータに対して前記所定の変換を施すステップ、および、該変換されたデータを暗号化するステップ、を含むことを特徴とする請求項８に記載の通信方法。

【請求項１１】　前記第２の端末から暗号化データを取得する工程の前後いずれかに、前記第２の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項８に記載の通信方法。

【請求項１２】　前記第１の端末に送信する工程の前後いずれかに、前記第１の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項８に記載の通信方法。

【請求項１３】　前記第１の端末に送信する工程の前後いずれかに、前記第１の端末からの認証・鍵交換要求を受け取る工程、および、前記第１の端末の利用者の認証ができた場合のみ、前記第１の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項８に記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、IEEE1394等の家庭網とインターネット等の公衆網を結合する通信装置に係り、特に、著作権保護を考慮して家庭網から公衆網にデータを送信する通信装置、およびその通信方法に関する。

【０００２】

【従来の技術】近年、情報のデジタル技術の進化に伴い、インターネットやホームネットワーク等が急速に普及して来ている。これにより、インターネット接続機能を持った家電機器や、家庭網とインターネットを接続する新しいゲートウェイ等、新しい市場が開けつつある。

【０００３】たとえば、IEEE1394等の家庭網（ホームネットワーク）とインターネット等の公衆網とを結び付けるホームゲートウェイに関しては、ストレージ（蓄積）機能を持たせたり、デジタル放送受信機能を持たせる等、多くのアイディアが存在する。その中でも特に、ホームネットワークからのオーディオ・ビジュアル・デー

タ(AVデータ)を受信し、その受信されたAVデータを、たとえばエムペグ－４(MPEG-4)等に圧縮した後、インターネット側に送信する、という注目すべきアイディアがある。これは、外出先から、家庭内のAVコンテンツを閲覧可能にしたり、家庭内の監視カメラによって撮影されたAVデータを、家庭外から参照可能にする等、多くのアプリケーションが考えられるからである。

【０００４】

【発明が解決しようとする課題】ホームネットワーク上を流れるAVデータには、映画や音楽、音声、テレビ番組等、の著作物が含まれている場合がある。もちろん、AVデータ自身が著作物である場合もある。このような著作物を含む、あるいは著作物自体であるAVデータは、著作権による保護のため、ホームネットワーク上では暗号化されて送信される場合が多い。このため、ホームネットワーク上で入手された、暗号化AVデータをインターネットに再送信する場合、暗号化AVデータを一旦復号し、その暗号化を解除する必要がある。しかし、その復号されたAVデータをそのまま暗号化せずに、インターネット側に送信したのでは、今度は、インターネット上における著作権保護の意味が失われてしまうことになる。

【０００５】一方、ホームゲートウェイが置かれている家庭の利用者以外からの、家庭内のAVコンテンツの閲覧・参照等の要求に対して、不用意に答えてしまうと、インターネットを介して不特定多数にコンテンツを送信してしまうことになりかねない。このことは、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則に反することになる。

【０００６】このように、従来においては、ホームネットワークからインターネットに供給される著作物の送信については、著作権保護の観点からは、未だ不十分である。

【０００７】本発明は、このような課題を解決し、家庭網から公衆網へデータを送信する際の著作権保護を実現する通信装置およびその通信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明は、第１の網（公衆網）１６と第２の網（家庭網、ローカルエリアネットワーク）１４の間に配置され、公衆網１６に接続された第１の端末（再生端末）２０と家庭網１４に接続された第２の端末（サーバー）１８の間で暗号化データを転送する通信装置であることを特徴とする。

【０００９】より詳細には、本発明の第１の特徴は、上記の通信装置であって、再生端末２０との間で、認証・鍵交換を実行する第１の認証・鍵交換部２４３と、サーバー１８との間で、認証・鍵交換を実行する第２の認証・鍵交換部２６１と、サーバー１８から得られた暗号化データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末２０に送信する送信部２２と、再生端末２０の利用者を認証し、その利用者の認証ができない場合には、再生端末２０との通信を拒絶する利用者認証部２４２と、から構成される通信装置であることを第１の特徴とする。ここで、「暗号化データ」とは、少なくとも一部に著作物を含む、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等であって、著作権法による保護のために暗号化されているものである。「所定の変換」とは、データ圧縮符号化方式およびデータ圧縮符号化速度のうちの少なくとも一方を変換することを意味する。より具体的には、家庭網１４上を流れる暗号化データのデータ圧縮符号化方式、符号化速度を、公衆網１６に適した符号化方式、符号化速度に、変換することである。「暗号制御情報」とは、サーバー１８から得られたデータの録画やコピーを制御する情報である。たとえば、これ以上コピーを認めないという“No More Copy”である。

【００１０】本発明の第１の特徴によれば、再生端末２０の利用者を認証することで、サーバー１８内のデータを要求する利用者が、正規の人物であることを十分に予想することができる。このため、利用者の認証以降の手順が、その利用者が個人的に楽しむための手順であることが明らかとなる。したがって、このことから、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則を遵守することが可能となる。

【００１１】さらに、あらかじめ付加されていた、“No More Copy”等の暗号制御情報を、再生端末２０に送信する際にも付加するので、元々のコピー制御の指定を守ることができる。このため、たとえば、録画やコピーをしてはいけない、と指定されていたデータは、再生端末２０に送信する際も、録画やコピーを未然に防止する形式にすることができる。

【００１２】本発明の第２の特徴は、上記の第１の特徴で述べた通信装置が実現する通信方法に係る。すなわち、第１の網（公衆網）１６に接続された第１の端末（再生端末）２０と第２の網（家庭網、ローカルエリアネットワーク）１４に接続された第２の端末（サーバー）１８との間で暗号化データを転送する通信方法であり、再生端末２０の利用者を認証する工程と、その利用者の認証ができた場合のみ、サーバー１８から暗号化データを取得する工程と、その取得された暗号化データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末２０に送信する工程と、を少なくとも含む通信方法であることである。

【００１３】

5

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【００１４】図１は、本発明の実施の形態に係る通信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。図１に示すように、本発明の実施の形態に係る通信装置１０は、家庭１２内に配設され、IEEE1394等で構成された家庭網１４と、家庭１２外に配設され、インターネット等で構成された公衆網１６と、の間に接続される。家庭網１４には、様々なAVデータを格納するサーバー１８が接続され、このサーバー１８内に蓄積されたAVデータは、通信装置１０によって、家庭網１４から公衆網１６に送信される。公衆網１６には、AVデータを再生することができる再生端末２０が接続され、この再生端末２０は、公衆網１６を介して、通信装置１０から送信されたAVデータを受信する。そして、再生端末２０は、その受信されたAVデータを、再生する。

【００１５】AVデータとしてはたとえば、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等が挙げられる。ここでは、説明の簡単化を図るため、AVデータの一部に著作物が含まれる、あるいはAVデータ自体が著作物であるとする。また、再生端末２０は、AVデータの種類によって、種々の形態を採りうるものであり、たとえばAVデータが映像であれば、再生端末２０はビューアとなる。もちろん、再生端末２０は、据え置き型のものであっても、持ち運びを前提にした携帯端末のいずれであっても構わない。

【００１６】図１では、家庭網１４および公衆網１６からなるネットワークには、３つの通信ノード、すなわち通信装置１０、サーバー１８および再生端末２０が接続されているが、これ以外の通信ノードが接続されていても、もちろん構わない。

【００１７】本発明の実施の形態に係る通信装置１０は、異種のネットワークである、家庭網１４と公衆網１６とを結合する、ホームゲートウェイの役目を担うものである。この通信装置１０の接続によって、異なる通信プロトコルを使っている家庭網１４と公衆網１６との間で、データのやりとりが可能となる。通信装置１０はたとえば、家庭網１４から公衆網１６へデータを送信する場合には、その送信されるデータを公衆網１６が使用するプロトコルと互換性のある形式に変換する。

【００１８】また、本発明の実施の形態に係る通信装置１０は、公衆網１６側から家庭網１４に接続された、サーバー１８や、デジタルAV機器（たとえばDVDプレーヤ、据置型VTR、カメラ一体型VTR等）（図示しない）、の制御を可能とする機能を備える。

【００１９】さらに、本発明の実施の形態に係る通信装置１０は、サーバー１８やデジタル機器から出力されたAVコンテンツを、リアルタイムにMPEG-4等の高圧縮のAVデータに変換し、その変換されたAVデータを公衆網１６側に送信する機能を備える。ここで、このような変換機能が備えられるのは、通常、家庭１２内に配設される家庭網１４と比べて、インターネット等の公衆網１６の通信帯域が非常に細く、このため、家庭網１４上のAVデータをそのまま公衆網１６に流すことはできないからである。したがって、たとえばIEEE1394からなる家庭網１４上でやりとりされるMPEG-2データは、MPEG-4データに変換された後に、公衆網１６に送信されることになる。

【００２０】さて、図１に示したネットワーク・システムでは、著作権保護のため、家庭網１４上でやりとりされるAVデータを暗号化処理する場合がある。本発明の実施の形態に係る通信装置１０は、暗号化処理されたAVデータについても、そのAVデータを家庭網１４から公衆網１６に送信する場合には、上記のようなMPEG-2符号からMPEG-4符号への変換を実行する。ここで、この符号変換の際には、暗号化されたAVデータは一旦復号される。そして、変換終了後、変換後のAVデータは、再び暗号化されて、公衆網１６側に送信されることになる。さらに、この実施の形態に係る通信装置１０は、AVデータの暗号化処理のため、上記の変換処理および暗号化・復号処理に先立って、家庭網１４側および公衆網１６側の両方との間で、認証・鍵交換処理を実行する。

【００２１】次に、図１および図２を用いて、本発明の実施の形態に係る通信装置１０の構成について説明する。図２は、本発明の実施の形態に係る通信装置１０の構成を示すブロック図である。図２では、説明の簡単化を図るため、図１の家庭網１４としてIEE1394バスを、公衆網１６としてインターネットを採用した場合を示す。さらに、IEEE1394バス１４からインターネット１６へのデータ送信の際、そのデータはMPEG-2符号からMPEG-4符号に変換されるものとする。

【００２２】図２に示すように、本発明の実施の形態に係る通信装置１０は、IEEE1394バス１４からインターネット１６に送信されるAVデータの符号変換および暗号化・復号を実行する送信部２２と、インターネット１６側との認証・鍵交換処理を実行する第１の認証・鍵交換部２４と、IEEE1394バス１４側との認証・鍵交換処理を実行する第２の認証・鍵交換部２６と、送信部２２および第１の認証・鍵交換部２４とインターネット１６との間を結ぶインターネットインターフェース２８と、送信部２２および第２の認証・鍵交換部２６とIEEE1394バス１４との間を結ぶIEEE1394インターフェース３０と、を備える。

【００２３】ここで、送信部２２は、IEEE1394インターフェース（以下、単に「IEEE1394I/F」と呼ぶ）３０と接続し、IEEE1394バス１４からのAVデータを受信する同期データ処理部２２１と、同期データ処理部２２１と接続し、受信されたAVデータを復号する復号処理部２２２

と、復号処理部２２２と接続し、復号されたAVデータ（MPEG-2データ）をMPEG-2符号からMPEG-4符号に変換する変換処理部２２３と、変換処理部２２３と接続し、MPEG-4符号に変換されたAVデータ（MPEG-4データ）を、再び暗号化する暗号化処理部２２４と、暗号化処理部２２４と接続し、暗号化されたAVデータをリアルタイムに、インターネットインターフェース（以下、単に「インターネットI/F」と呼ぶ）２８を介して、インターネット１６側に送信するリアルタイムトランスポートプロトコル(RTP)処理部２２５と、から構成される。

【００２４】第１の認証・鍵交換部２４は、インターネット１６を介して、サーバー１８内に蓄積された映像や音楽等のAVコンテンツの閲覧・参照等を要求する、各利用者の再生端末２０に、識別ＩＤ（利用者ID）およびパスワード入力用ダイアログ画面を備えた利用者認証用ホームページおよびIEEE1394バス１４に接続されたサーバー１８や家電機器等を遠隔制御するため遠隔制御用ホームページを含む、各種のホームページを送信するホームページ処理部２４１と、利用者認証用ホームページのダイアログ画面から入力された利用者IDおよびパスワードが正規のものであるか否かを照合する利用者認証処理部２４２と、正規の利用者の再生端末２０との間で認証・鍵交換処理を実行する第１の認証・鍵交換処理部２４３と、再生端末２０とのやりとりをTCPパケット化するためのTCP処理部２４４と、から構成される。

【００２５】第２の認証・鍵交換部２６は、サーバー１８との間で認証・鍵交換処理を実行する第２の認証・鍵交換処理部２６１と、サーバー１８とのやりとりを非同期パケット化するための非同期データ処理部２６２と、から構成される。

【００２６】次に、図３乃至図５を参照して、本発明の実施の形態に係る通信装置１０の動作について説明する。図３は、本発明の実施の形態に係る通信装置１０と、サーバー１８および再生端末２０と、の間の処理シーケンスチャートであり、図４および図５は、本発明の実施の形態に係る通信方法の処理手順を示すフローチャートである。

【００２７】（１）図３のステップＳ１０１において、まず、再生端末２０が、インターネット１６を介して、通信装置１０に対して、サーバー１８内のデータを閲覧・参照するための遠隔制御用ホームページを要求する（図４のステップＳ２０１）。この遠隔制御用ホームページには、IEEE1394バス１４に接続された、サーバー１８や各種の家電機器を遠隔制御するためのボタンが少なくとも表示される。このボタンは、たとえばグラフィカルユーザインターフェース（Graphical User Interface; GUI）で構成される。

【００２８】（２）図３のステップＳ１０２において、再生端末２０からの遠隔制御用ホームページ要求を受けた通信装置１０は、再生端末２０に利用者認証用ホームページを送信し、利用者IDおよびパスワードを要求する（図４のステップＳ２０２）。通信装置１０は、この利用者IDおよびパスワードを要求し、ホームページを要求する再生端末２０に利用者が、正規の利用者であるか否かを判断する。すなわち、要求されたホームページは、サーバー１８や家電機器等の遠隔制御を可能とするものであり、正規の利用者以外にこのホームページを与えてしまうと、不審な人物にサーバー１８や家電機器の制御をされかねない。そこで、通信装置１０は、遠隔制御用ホームページを要求する再生端末２０に対して、利用者IDおよびパスワードの入力を要求し、その利用者があらかじめ登録された、怪しくない人物であるか否かを確認する。

【００２９】（３）図３のステップＳ１０３において、利用者IDおよびパスワードの入力を要求された再生端末２０の利用者は、たとえば再生端末２０に設けられたダイヤルキーを用いて、利用者ＩＤおよびパスワードを入力する。再生端末２０に入力された利用者IDおよびパスワードは、インターネット１６を経由して、通信装置１０に送信される。

【００３０】（４）図３のステップＳ１０４において、再生端末２０から送信された利用者IDおよびパスワードを受け取った通信装置１０は、たとえば正規の利用者の利用者IDおよびパスワードを格納するデータベースを有している。そして、通信装置は、受け取った利用者IDおよびパスワードがそのデータベースに登録されているか否かを照合する（図４のステップＳ２０３）。利用者IDおよびパスワードが登録されていなければ（図４のステップＳ２０３ＮＯ）、直ちに、再生端末２０との回線を切断する（図５のステップＳ２０４）。

【００３１】（５）利用者IDおよびパスワードが登録されていれば（図４のステップＳ２０３ＹＥＳ）、図３のステップＳ１０５において、通信装置１０は遠隔制御用ホームページを、インターネット１６を介して、再生端末２０に送信する（図５のステップＳ２０５）。そして、再生端末２０の利用者は、遠隔制御用ホームページに表示された、サーバー１８の制御用ボタンを操作することで、たとえば図６に示すようなコンテンツ選択画面を取得する。図６に示すように、このコンテンツ選択画面３２には、「ホームサーバーに録画されている番組は以下の通りです。」と表示されており、利用者は、この選択画面３２から、サーバー１８内のコンテンツの再生が可能となる。すなわち、この選択画面３２には、各コンテンツに対応付けられた、複数のボタン３４（「ドラマ」３４ａ、「スポーツ」３４ｂ、「ニュース」３４ｃ、「プライベートビデオ１」３４ｄ、「プライベートビデオ２」３４ｅ）が表示されており、各ボタン３４を操作することで、各ボタン３４に対応付けられたコンテンツを再生させることができる。なお、遠隔制御用ホームページを取得した利用者は、その遠隔制御用ホームペ

ージの取得という事実によって、以降の手続きにおいては、IEEE1394バス１４が配設された家庭１２の住人と見なすことができる。

【００３２】（６）図３のステップＳ１０６において、再生端末２０に利用者が、たとえば「ドラマ」の再生を要求した場合、つまりボタン３４ａを操作すると（図４のステップＳ２０６）、図３のステップＳ１０７において、そのコンテンツ要求を受けた通信装置１０は、サーバ１８に、IEEE1394バス１４を介して、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、コンテンツ送信要求のコマンドを発行する（図４のステップＳ２０７）。

【００３３】（７）図３のステップＳ１０８において、コンテンツ「ドラマ」の送信要求を受けたサーバー１８は、第１の暗号化鍵K1で暗号化されたコンテンツ「ドラマ」（MPEG-2データ）を、IEEE1394バス１４を介して、通信装置１０に送信する（図４のＳ２０７）。ここで、このコンテンツ「ドラマ」に書き込まれた暗号制御情報は、新たにこれ以上コピーを認めないという“No More Copy”であるとする。たとえば、IEEE1394における暗号化方式のデファクトスタンダードであるデジタルトランスミッションコンテンツプロテクション（DTCP）である。なお、暗号化されたAVデータ（コンテンツ「ドラマ」）は、IEEE1394バス上の同期チャネルを通して送信される。

【００３４】（８）図３のステップＳ１０９において、暗号化AVデータ（MPEG-2データ）を受信した通信装置１０は、そのAVデータの暗号化の事実により、認証・鍵交換が必要であることを認識する。そして、通信装置１０は、サーバー１８との間で、認証・鍵交換処理を実行する（図４のステップＳ２０９）。この認証・鍵交換処理によって、通信装置１０は、暗号化AVデータの復号のために必要な第１の復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、第１の復号鍵は第１の暗号化鍵K1と同一である。

【００３５】（９）図３のステップＳ１１０において、第１の復号鍵K1を入手した通信装置１０は、先に受信したAVデータを復号する（図４のステップＳ２１０）。

【００３６】（１０）図３のステップＳ１１１において、抽出されたMPEG-2データであるAVデータを、MPEG-4データに変換して再圧縮する（図５のステップＳ２１１）。ここではMPEG-2/MPEG-4変換を実行しているが、他の例として、たとえばMPEG-2データの符号化速度を、インターネット１６の通信帯域に適合するように、“絞る”、という形式を採っても良い。

【００３７】（１１）図３のステップＳ１１２において、通信装置１０は、MPEG-4符号に変換されたAVデータを、第２の暗号化鍵K2を用いて再び暗号化する（図５のステップＳ２１２）。ここで、このAVデータは、元々暗号制御情報“No More Copy”が書き込まれたコンテンツである。すなわち、録画やコピーが禁止されたデータは、再送出の際にも、やはり録画やコピーを未然に防ぐ形式で送信されるべきである。したがって、変化された後でも、このAVデータには“No More Copy”が書き込まれることになる。また、この再暗号化が、図３のステップＳ１０２～Ｓ１０５の後に実行されるのは、最初にパスワード入力等によって、再生端末２０の利用者が正規の利用者であると十分に予想され、このため、以降の手順が、利用者が個人的に楽しむための手順であることが明らかとなるからである。

【００３８】（１２）図３のステップＳ１１３において、通信装置１０は、再暗号化されたAVデータ（MPEG-4データ）を、インターネット１６を介して、再生端末２０に送信する（図５のステップＳ２１３）。転送プロトコルとしてはRTPが利用される。また、再暗号化されたAVデータには、上述したように、暗号制御情報“No More Copy”が書き込まれる。したがって、再生端末２０は、受け取ったAVデータを不正に蓄積することは不可能となる。

【００３９】（１３）図３のステップＳ１１４において、再暗号化AVデータ（MPEG-4データ）を受信した再生端末２０は、そのAVデータの暗号化の事実により、認証・鍵交換が必要であることを認識する。そして、再生端末２０は、通信装置１０との間で、認証・鍵交換処理を実行する。この認証・鍵交換処理によって、再生端末２０は、再暗号化AVデータの復号のために必要な第２の復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、第２の復号鍵は第２の暗号化鍵K2と同一である。この再生端末２０と通信装置１０とのやりとりは、たとえばTCPパケットの形で行われる。

【００４０】ここで、通信装置１０は、再生端末２０から認証・鍵交換処理要求を受けた場合（図５のステップＳ２１５）、その再生端末２０の利用者が、図３のステップＳ１０２～Ｓ１０５の利用者認証によって、正規の利用者であると判断された者であるか否かを調べることが望ましい（図５のステップＳ２１５）。正規の利用者でない場合、インターネット１６を介して、不特定多数にコンテンツを送信してしまうことになりかねず、著作権法で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則に反するからである。図５のステップＳ２１５は、このようなことを未然に防止することが可能となる。もちろん、正規の利用者でなければ（図５のステップＳ２１５ＮＯ）、通信装置１０は、直ちに、再生端末２０との回線を切断する（図５のステップＳ２０４）。

【００４１】このようにして、正規の利用者の再生端末２０は、第２の復号鍵K2を他人に知られること無く取得することができ、受信された再暗号化AVデータを復号できる。ただし、上述したように、AVデータには“No More Copy”が書き込まれているので、再生端末２０は、そ

11

のAVデータを蓄積／コピーすることはできない。その場で、デコード／表示させることができるだけである。

【００４２】このように、本発明の実施の形態によれば、家庭網上で入手された、チャンネル作物を含む、あるいは著作物自体のAVデータを、公衆網に送信する場合に、その著作物の著作権法による保護を確実に実現することができる。

【００４３】特に、近年のデジタル化・ネットワーク化の進展により、ネットワーク上で著作物を送信するという著作物の利用方法が発達・普及する現状にあっては、本発明の重要性はきわめて高いものである。

【００４４】

【発明の効果】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信装置を実現できる。

【００４５】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信方法を実現できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る通信装置によって接続された、家庭網と公衆網とからなるネットワーク・システムの全体構成を示すブロック図である。

【図２】本発明の実施の形態に係る通信装置の具体的な構成を示すブロック図である。

【図３】本発明の実施の形態に係る通信装置、サーバーおよび再生端末間で、著作物を含むAVデータを送受信する際の、処理シーケンスチャートである。

【図４】本発明の実施の形態に係る通信装置の通信方法の処理手順を示すフローチャートである（その１）。

【図５】本発明の実施の形態に係る通信装置の通信方法＊の処理手順を示すフローチャートである（その２）。

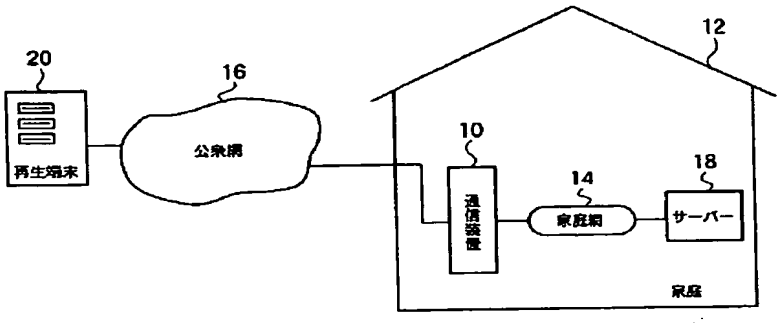
12

【図６】本発明の実施の形態に係る通信装置から、再生端末に送信される、コンテンツ選択画面の内容を示す図である。

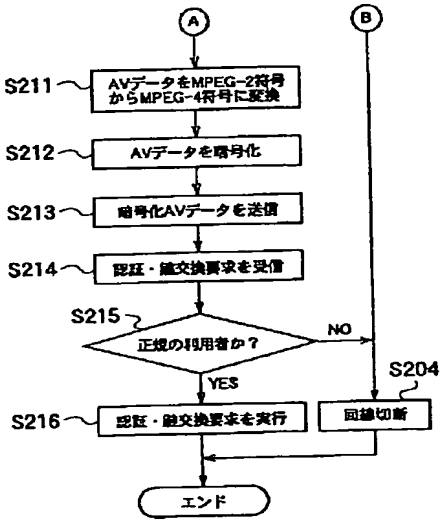
【符号の説明】

１０　通信装置
１２　家庭
１４　家庭網
１６　公衆網
１８　サーバー
２０　再生端末
２２　送信部
２４　第１の認証・鍵交換部
２６　第２の認証・鍵交換部
２８　インターネットインターフェース
３０　IEEE1394インターフェース
３２　コンテンツ選択画面
３４　ボタン
２２１　同期データ処理部
２２２　復号処理部
２２３　変換処理部
２２４　暗号化処理部
２２５　RTP処理部
２４１　ホームページ処理部
２４２　利用者認証処理部
２４３　第１の認証・鍵交換処理部
２４４　TCP処理部
２６１　第２の認証・鍵交換処理部
２６２　非同期データ処理部

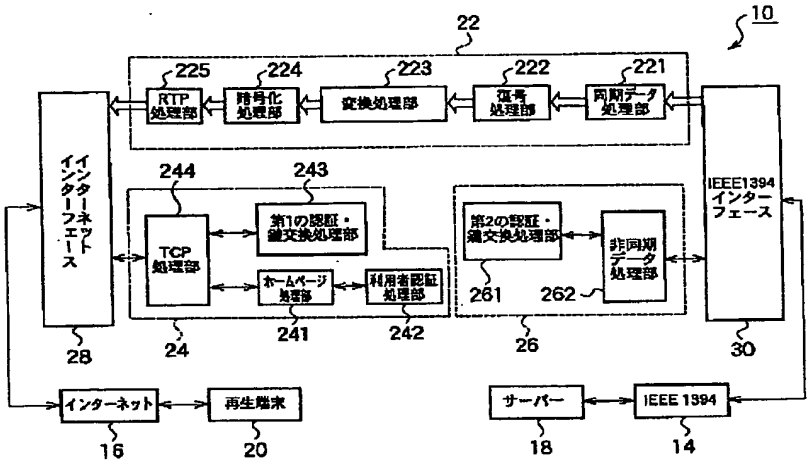
【図１】



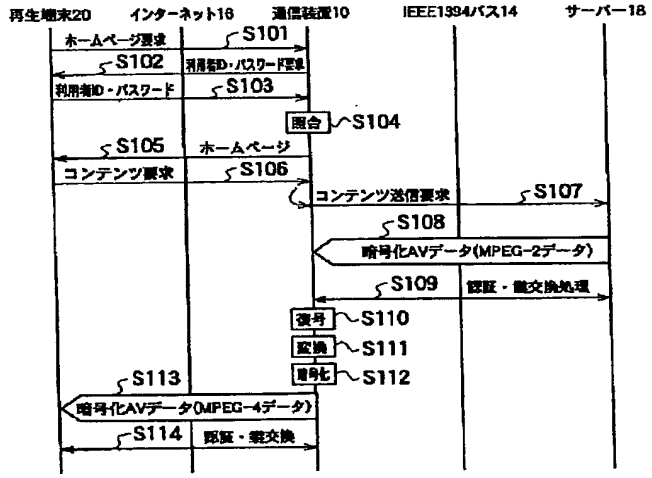
【図５】



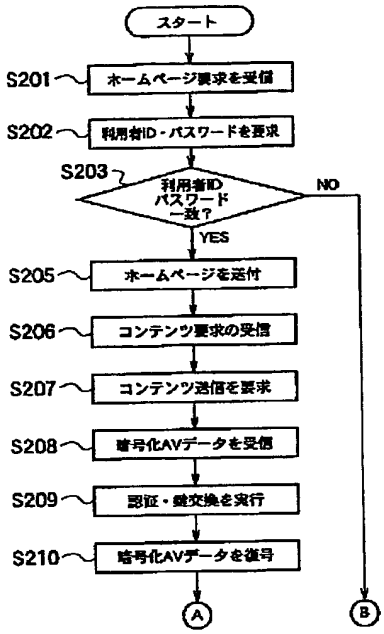
【図２】


22
10
225
224
223
222
221
RTP処理部
暗号化処理部
変換処理部
復号処理部
同期データ処理部
インターフェース
IEEE1394インターフェース
244
243
TCP処理部
第1の認証・鍵交換処理部
ホームページ処理部
利用者認証処理部
第2の認証・鍵交換処理部
非同期データ処理部
261
262
28
24
241
242
26
30
インターネット
再生端末
サーバー
IEEE 1394
16
20
18
14

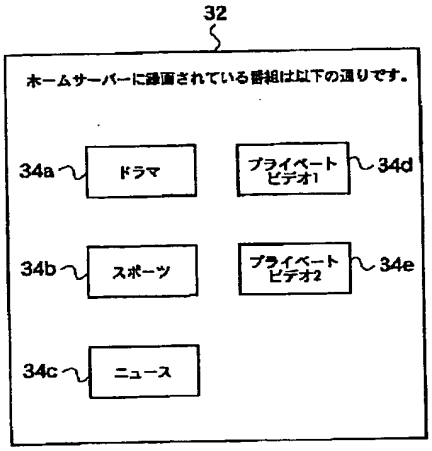
【図３】


再生端末20
インターネット16
通信装置10
IEEE1394バス14
サーバー18
ホームページ要求
S101
S102
利用者ID・パスワード要求
利用者ID・パスワード
S103
照合
S104
S105
ホームページ
コンテンツ要求
S106
コンテンツ送信要求
S107
S108
暗号化AVデータ(MPEG-2データ)
S109
認証・鍵交換処理
復号
S110
変換
S111
暗号化
S112
S113
暗号化AVデータ(MPEG-4データ)
S114
認証・鍵交換

【図４】


スタート
S201
ホームページ要求を受信
S202
利用者ID・パスワードを要求
S203
利用者ID パスワード 一致?
NO
YES
S205
ホームページを送付
S206
コンテンツ要求の受信
S207
コンテンツ送信を要求
S208
暗号化AVデータを受信
S209
認証・鍵交換を実行
S210
暗号化AVデータを復号
A
B

【図６】


32
ホームサーバーに録画されている番組は以下の通りです。
34a
ドラマ
プライベートビデオ1
34d
34b
スポーツ
プライベートビデオ2
34e
34c
ニュース

フロントページの続き

Ｆターム(参考) 5J104 AA07 AA13 BA02 EA04 EA15
KA01 NA02 NA05
5K030 GA15 HB01 HB02 HC01 HC14
HD01 HD06
5K033 AA08 BA01 BA11 CB08 DA06
DA11 DA13 DB10 DB18
9A001 BB04 CC07 CC08 EE03 EE04
JJ25 JJ27 KK56 LL03

THIS PAGE BLANK (USPTO)